AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

1. (currently amended): An identification system comprising:

a plurality of end terminals, ~~each of the end terminals transmitting a transaction request message containing biometrics data of a user and a user identifier of said user to a communications network~~;

~~at least one~~ a plurality of electronic commerce service provider (ECSP) units, wherein each one of the plurality of ECSP units ~~for receiving said~~ receives a transaction request message containing ciphered biometrics data of a user and a user identifier of said user transmitted from the plurality of end terminals via ~~said~~ a communications network and ~~transmitting~~ for each received transaction request message, one of the plurality of ECSP units transmits an authentication request message containing said ciphered biometrics data and said user identifier to said network; and

an authentication server ~~having~~ comprising a database for mapping a plurality of registered biometrics data to a plurality of corresponding registered user identifiers, wherein the authentication server ~~receiving~~ receives the authentication request messages from the plurality of ECSP units via said network, ~~comparing~~ and for each of the received authentication request messages, the authentication server decipheres the ciphered biometrics data and compares the ~~received~~ deciphered biometrics data to one of the registered biometrics data which is mapped in

said database to the user identifier contained in ~~said~~ the received authentication request message and ~~returning~~ returns a reply to ~~said~~ the plurality of ECSP units via said network indicating that said transaction request message is authenticated if the received biometrics data coincides with said mapped biometrics data.

2. (canceled).

3. (currently amended): The identification system of claim 1, wherein ~~said~~ each one of the plurality of ECSP units includes a conversion table for mapping a first plurality of user identifiers to a second plurality of user identifiers, wherein said first plurality of user identifiers are used by said plurality of end terminals and said second plurality of user identifiers are the user identifiers registered in said database, ~~said~~ each one of the plurality of ECSP units ~~converting~~ converts the user identifier contained in the received transaction request message to one of the second plurality of user identifiers which is mapped to the received user identifier and ~~transmitting~~ transmits said authentication request message containing the converted user identifier.

4. (currently amended): The identification system of claim 1, wherein each of said end terminals is configured to ~~cipher the~~ generate said ciphered biometrics data with a secret key generated by a variable secret key generator which generates secret keys which vary with time, the generated secret key being agreed-upon with said authentication server.

5. (currently amended): The identification system of claim 4, wherein said variable secret key generator is located at said authentication server and wherein each of said end terminals is configured to transmit a key request message to said authentication server via said plurality of ECSP units, to receive said secret key from the secret key generator, and to ciphering ~~the~~ a biometrics data with the received secret key before said transaction request message is transmitted.

6. (original): The identification system of claim 5, wherein said authentication server comprises a variable secret key generator which generates a secret key which varies with time , and a decryption unit for deciphering the received ciphered biometrics data by using the secret key generated by said secret key generator.

7. (original): The identification system of claim 1, wherein each of said end terminals comprises a user terminal exclusively owned by said user.

8. (currently amended): The identification system of claim 1, wherein each of said end terminals comprises a sales terminal to which a plurality of user's handheld personal units can be connected, wherein said sales terminal transparently transmits a transaction request messaged received from each of the personal units to said plurality of ECSP units.

9. (original): The identification system of claim 1, wherein said biometrics data of said user is a fingerprint of said user.

10. (original): The identification system of claim 1, wherein said biometrics data of said user is an extracted feature of a fingerprint of said user.

11. (currently amended): An identification system comprising:

a plurality of end terminals ~~respectively identified by user identifiers, each of the end terminals transmitting a transaction request message containing biometrics data of a user to a communications network~~;

~~at least one~~ a plurality of electronic commerce service provider (ECSP) units, wherein each one of the plurality of ECSP units ~~for receiving said~~ receives a transaction request message containing ciphered biometrics data of a user and a user identifier of said user transmitted from the plurality of end terminals via ~~said~~ a communications network and ~~transmitting~~ for each

received transaction request message, one of the plurality of ECSP units transmits an authentication request message containing said ciphered biometrics data to said network; and

an authentication server ~~having~~ comprising a database for mapping a plurality of registered biometrics data to a plurality of corresponding registered user identifiers, wherein the authentication server ~~receiving~~ receives the authentication request messages from the plurality of ECSP units via said network, ~~comparing~~ and for each of the received authentication request messages, the authentication server deciphers the ciphered biometrics data and compares the ~~received~~ deciphered biometrics data to all of the registered biometrics data in said database, ~~detecting~~ detects the user identifier mapped to the registered biometrics data which coincides with the ~~received~~ deciphered biometrics data, and ~~returning~~ returns a reply to ~~said~~ the plurality of ECSP units via said network indicating that a user identified by the detected user identifier is authenticated.

12. (canceled).

13. (currently amended): The identification system of claim [[12]] 11, wherein each of said end terminals is configured to ~~cipher the~~ generate said ciphered biometrics data with a secret key generated by a variable secret key generator which generates secret keys which vary with time, the generated secret key being agreed-upon with said authentication server.

14. (currently amended): The identification system of claim 13, wherein said variable secret key generator is located at said authentication server and wherein each of said end terminals is configured to transmit a key request message to said authentication server via said plurality of ECSP units to receive said secret key from the secret key generator, and to ciphering ~~the~~ a biometries data with the received secret key before said transaction request message is transmitted.

15. (original): The identification system of claim 14, wherein said authentication server comprises a variable secret key generator which generates a secret key which varies with time, and a decryption unit for deciphering the received ciphered biometrics data by using the secret key generated by said variable secret key generator.

16. (currently amended): The identification system of claim [[12]] 11, wherein each of said end terminals comprises a user terminal exclusively owned by said user.

17. (currently amended): The identification system of claim [[12]] 11, wherein each of said end terminals comprises a sales terminal to which a plurality of user's handheld personal units can be connected, wherein said sales terminal transparently transmits a transaction request messaged received from each of the personal units to said plurality of ECSP units.

18. (original): The identification system of claim [[12]] 11, wherein said biometrics data of said user is a fingerprint of said user.

19. (original): The identification system of claim [[12]] 11, wherein said biometrics data of said user is an extracted feature of a fingerprint of said user.

20. (currently amended): An identification method comprising the steps of:

a) transmitting, from ~~an~~ a plurality of end terminals, ~~a~~ transaction request messages, containing ciphered biometrics data of a user to a communications network;

b) receiving, at ~~an~~ each one of a plurality of electronic commerce service providers, ~~said~~ one of the transaction request messages via said network;

c) for each received transaction request message, transmitting ~~, from the electronic commerce service provider,~~ an authentication request message containing said ciphered biometrics data from one of the plurality of electronic commerce service provider units to said network;

d) receiving said authentication request messages via said network at a user authenticator having a database for storing a plurality of registered biometrics data and deciphering the ciphered biometrics data contained in the received authentication request messages;

e) for each of the received authentication request messages, determining whether the ~~received~~ deciphered biometrics data has corresponding biometrics data in said database; and

f) for each of the received authentication request messages, returning a reply from said user authenticator to said plurality of electronic commerce service providers via said network indicating that said transaction request message is authenticated if the ~~received~~ deciphered biometrics data coincides with one of the registered biometrics data of the database.

21. (canceled).

22. (currently amended): An identification method comprising the steps of:

a) transmitting, from ~~an~~ a plurality of end terminals, ~~a~~ transaction request messages, each transaction request message containing ciphered biometrics data of a user and a user identifier of said user to a communications network;

b) receiving, at ~~an~~ each one of a plurality of electronic commerce service providers, one of said transaction request messages via said network;

c) for each of the received transaction request messages, transmitting ~~from the electronic commerce service provider,~~ an authentication request message containing said ciphered biometrics data and said user identifier from one of the plurality of electronic commerce service provider units to said network;

d) receiving said authentication request messages at a user authenticator via said network, the authenticator having a database in which a plurality of registered biometrics data are mapped to a plurality of corresponding registered user identifiers and deciphering the ciphered biometrics data contained in the received authentication request messages;

e) for each of the received authentication request messages, comparing the ~~received~~ deciphered biometrics data to one of the registered biometrics data which is mapped in said database to the user identifier contained in said authentication request message; and

f) for each of the received authentication request messages, returning, from the user authenticator, a reply to said plurality of electronic commerce service providers via said network indicating that said transaction request message is authenticated if the received biometrics data coincides with said mapped biometrics data.

23. (currently amended): The identification method of claim 22, wherein the user identifiers stored in said database are different from the user identifiers of said end terminals, further comprising converting, at ~~said~~ each one of the plurality of electronic commerce service providers, the user identifier contained in the received transaction request message to a second user identifier which is contained in said authentication request message as the first-mentioned user identifier.

24. (canceled).

25. (currently amended): The identification method of claim [[24]] 22, wherein ~~the~~ a biometrics data contained in the transaction request message is ciphered by using a secret key which varies with time and agrees with the secret key with which the ciphered biometrics data is deciphered at said user authenticator.

26. (currently amended): An identification method comprising the steps of:

a) transmitting, from ~~an~~ a plurality of end terminals, ~~a~~ transaction request messages, each transaction request message containing ciphered biometrics data of a user to a communications network;

b) receiving, at ~~an~~ each one of a plurality of electronic commerce service providers, one of said transaction request message via said network;

c) for each of the received transaction request messages, transmitting, ~~from said service provider,~~ an authentication request message containing said ciphered biometrics data from one of the plurality of electronic commerce service providers to said network;

d) receiving, at a user authenticator having a database in which a plurality of registered biometrics data are mapped to a plurality of corresponding registered user identifiers, said authentication request messages via said network and deciphering the ciphered biometrics data contained in the received authentication request messages;

e) for each of the received authentication request messages, comparing the ~~received~~ deciphered biometrics data to all of the registered biometrics data in said database to detect coincidence;

f) for each of the received authentication request messages, detecting the user identifier mapped to the biometrics data which coincides with the ~~received~~ deciphered biometrics data; and

g) for each of the received authentication request messages, returning a reply from the user authenticator to said plurality of electronic commerce service providers via said network indicating that said user having the detected user identifier is authenticated.

27. (canceled).

28. (currently amended): An identification system comprising:

a plurality of end terminals, ~~each of the end terminals transmitting to a communications network a registration request message and a transaction request message, each of said messages containing biometrics data of a user and a user identifier of said user~~;

~~at least one~~ a plurality of electronic commerce service provider (ECSP) units, wherein each one of the plurality of ECSP units receives a ~~for receiving said~~ registration request message containing ciphered biometrics data of a user and a user identifier of said user transmitted from the plurality of end terminals via ~~said~~ a communications network, retransmits ~~to retransmitting~~

the registration request message to said network, ~~and receiving~~ receives a ~~said~~ transaction request message containing said ciphered biometrics data and user identifier transmitted from the plurality of end terminals via said network, and ~~transmitting~~ for each received transaction request message, transmits an authentication request message containing said biometrics data and said user identifier to said network; and

an authentication server for receiving said registration request messages from said plurality of ECSP units via said network, mapping in a database a plurality of biometrics data contained in a plurality of said registration request messages to a plurality of corresponding user identifiers contained in said registration request messages, the authentication server further receiving the authentication request messages from the plurality of ECSP units via said network, and for each of the received authentication request messages, the authentication server deciphers the ciphered biometrics data and compares ~~comparing~~ the ~~received~~ deciphered biometrics data to one of the biometrics data which is mapped in said database to the user identifier contained in ~~said~~ the received authentication request message and ~~returning~~ returns a reply to said the plurality of ECSP units via said network indicating that said transaction request message is authenticated if the received biometrics data coincides with said mapped biometrics data.

29. (currently amended): An identification system comprising:

a plurality of end terminals, ~~each of the end terminals transmitting a registration request message containing biometrics data of a user and a user identifier of the user to a~~

~~communications network and transmitting a transaction request message containing said biometrics data to the communications network~~;

~~at least one~~ a plurality of electronic commerce service provider (ECSP) units, wherein each one of the plurality of ECSP units receives a ~~for receiving said~~ registration request message containing ciphered biometrics data of a user and a user identifier of said user transmitted from the plurality of end terminals via ~~said~~ a communications network, retransmits ~~to retransmitting~~ the registration request message to said network, ~~and receiving~~ receives a ~~said~~ transaction request message containing said ciphered biometrics data transmitted from the plurality of end terminals via said network, and ~~transmitting~~ for each received transaction request message, transmits an authentication request message containing said ciphered biometrics data and said user identifier to said network; and

an authentication server for receiving said registration request messages from said plurality of ECSP units via said network, mapping a plurality of biometrics data contained in a plurality of said registration request messages to a plurality of corresponding user identifiers contained in said registration request messages, the authentication server receiving the authentication request messages from the plurality of ECSP units via said network, and for each of the received authentication request messages, the authentication server decipheres the ciphered biometrics data and compares ~~comparing~~ the ~~received~~ deciphered biometrics data to all of the biometrics data in said database, ~~detecting~~ detects the user identifier mapped to the biometrics data which coincides with the received biometrics data, and ~~returning~~ returns a reply

to said plurality of ECSP units via said network indicating that a user identified by the detected user identifier is authenticated.

30. (new): An authentication server comprising:

a database for mapping a plurality of registered biometrics data to a plurality of corresponding registered user identifiers;

an interface unit for receiving authentication request messages from a plurality of electronic commerce service provider (ECSP) units via a network, each authentication request message containing biometrics data of a user and a user identifier of said user; and

a processor, wherein for each of the received authentication request messages, the processor compares the received biometrics data to one of the registered biometrics data which is mapped in said database to the user identifier contained in the received authentication request message,

wherein the interface unit returns a reply to the plurality of ECSP units via said network indicating that the transaction request message is authenticated if the received biometrics data coincides with the said mapped biometrics data,

wherein each authentication request message corresponds to a transaction request message transmitted to one of the plurality of ECSP units from one of a plurality of user terminals via said network.

31. (new): An authentication server comprising:

a database for mapping a plurality of registered biometrics data to a plurality of corresponding registered user identifiers;

an interface unit for receiving authentication request messages from a plurality of electronic commerce service provider (ECSP) units via a network, each authentication request message containing biometrics data of a user and a user identifier of said user; and

a processor, wherein for each of the received authentication request messages, the processor compares the received biometrics data to all of the registered biometrics data in said database and detects the user identifier mapped to the biometrics data which coincides with the received biometrics data,

wherein the interface unit returns a reply to the plurality of ECSP units via said network indicating that a user identified by the detected user identifier is authenticated,

wherein each authentication request message corresponds to a transaction request message transmitted to one of the plurality of ECSP units from one of a plurality of user terminals via said network.